

CS 2401
Complexity Theory
ASSIGNMENT # 2
DUE DATE: Dec 8, 2015

1. For this question, we will be interested in Boolean circuits over the complete basis, AND, OR and NEG. A counting argument due to Shannon shows that almost all Boolean functions on n inputs requires exponential circuit size. (That is, circuits of size at least $2^{\epsilon n}$ for some $\epsilon < 1$.) State and prove this theorem. Your proof should involve two steps. First, give a lower bound on the total number of distinct Boolean functions on n inputs. Secondly, give an upper bound on the total number of distinct Boolean functions that can be computed by Boolean circuits of a given size.
2. Prove the following statement. Let $MAX(n)$ be the maximum circuit size over all Boolean functions on n inputs. Suppose that every language in EXP can be computed by a family of Boolean circuits, where each circuit on n inputs is of size strictly less than $MAX(n)$. Then $P \neq NP$.

(Aside: This is quite interesting since it means that if we could resolve the maximal circuit size over all languages in EXP, then we will have proven a highly nontrivial lower bound. That is, either (1) all functions in EXP have small circuits, and then we have proven that $P \neq NP$, or (2) some language L in EXP requires large circuits. Stated another way, either proving superpolynomial circuit lower bounds for NP or proving submaximum circuit upper bounds for EXP would yield the same negative answer to the P versus NP question.)
3. Give the smallest size AC_d^0 circuit that you can for computing the parity function on inputs x_1, \dots, x_n . (The size should depend on d .)
4. Prove that if f is computed by a circuit of size S , then f is computed by fanout-2 circuit of size $O(S)$. (That is, without loss of generality, we can assume that the fanout of each gate is at most 2.)
5. $MED(x, y)$ is defined to be the median of the multiset $x \cup y$. Using binary search, one can show that $D(MED) = O(\log^2 n)$. Give an $O(\log n)$ -bit communication protocol for MED.
6. $GT(x, y)$, the greater-than function, is 1 if and only if $x > y$. What is the communication complexity of the greater-than function?
 - (a) Prove a lower bound of n on the deterministic communication complexity of GT .
 - (b) Given an upper bound of $O(\log n \log \log n)$ on the randomized complexity in the public coin model. (Hint: First try to get an $O(\log^2 n)$ algorithm and then improve it.)